Patrick. R. Leverty, Esq., NV Bar No . 8840
pat@levertylaw.com
William R. Ginn, Esq., NV Bar No. 6989
bill@levertylaw.com
LEVERTY & ASSOCIATES LAW, CHTD.
832 Willow Street
Reno, NV 89502
Telephone: (775)322-6636

William B. Federman (pro hac vice application forthcoming)
wbf@federmanlaw.com
Kennedy M. Brian (pro hac vice application forthcoming)
kpb@federmanlaw.com
FEDERMAN & SHERWOOD
10205 N. Pennsylvania Ave.
Oklahoma City, OK 73120
Telephone: (405) 235-1560

Attorneys for: *Plaintiff Class*

UNITED STATES DISTRICT COURT

DISTRICT OF NEVADA

KEVIN MEAGHER, on behalf of himself and on behalf of all other similarly situated individuals, Plaintiff vs. DIGITAL TRUST, LLC F/K/A THE KINGDOM TRUST COMPANY, Defendants	Case No.: 2:24-cv-1630 **CLASS ACTION COMPLAINT** **JURY TRIAL DEMANDED**

Plaintiff Kevin Meagher ("Plaintiff"), individually and on behalf of all other similarly situated individuals (the "Class" or "Class Members," as defined below), by and through his undersigned counsel, files this Class Action Complaint against Digital Trust, LLC f/k/a The Kingdom Trust Company (collectively referred to herein as "Digital Trust," "Kingdom Trust," or "Defendant") and alleges the following based on personal knowledge of facts, upon

information and belief, and based on the investigation of his counsel as to all other matters.

I. NATURE OF THE ACTION

1. Plaintiff brings this class action lawsuit against Digital Trust for its negligent failure to protect and safeguard Plaintiff's and the Class's highly sensitive personally identifiable information ("PII"). As a result of Digital Trust's negligence and insufficient data security, cybercriminals easily infiltrated Defendant's inadequately protected computer systems and stole the PII of Plaintiff and the Class (the "Data Breach" or "Breach"). Now, Plaintiff's and the Class's PII is in the hands of cybercriminals who will undoubtedly use their PII for nefarious purposes for the rest of their lives.

2. The number of individuals impacted by the data breach has yet to be disclosed but Notice of Data Breach Letters were at least sent to Data Breach victims in Iowa, North Carolina, the District of Colombia, and Rhode Island.[1]

3. According to Kingdom Trust, which is now known as Digital Trust, LLC, on or around March 1, 2024, Kingdom Trust become aware of potential unauthorized access to its network. [2]

4. After an investigation, Defendant definitively determined "certain data was subject to unauthorized access."[3]

5. Specifically, Defendant confirmed "personal information" may have been copied from its network.[4]

6. The PII stolen in the Data Breach included highly sensitive private information such as: names and Social Security numbers (collectively, "Private Information").[5]

7. Defendant began sending Notice of Data Breach Letters to victims of the Data Breach in

---

[1] *See* Exhibit 1 (Sample Notice of Data Breach Letter); Exhibit 2 (Plaintiff's Notice of Data Breach Letter).
[2] https://oag.ca.gov/ecrime/databreach/reports/sb24-590671.
[3] *Id.*
[4] Ex. 1.
[5] Ex. 2.

or around July or August 2024.[6]

8. Due to Defendant's negligence, cybercriminals have stolen and obtained everything they need to commit identity theft and wreak havoc on the financial and personal lives of thousands of individuals.

9. Now, and for the rest of their lives, Plaintiff and the Class Members will have to deal with the danger of identity thieves possessing and misusing their Private Information. Even those Class Members who have yet to experience identity theft have to spend time responding to the Breach and are at an immediate and heightened risk of all manners of identity theft as a direct and proximate result of the Data Breach. Plaintiff and Class Members have incurred and will continue to incur damages in the form of, among other things, identity theft, attempted identity theft, lost time and expenses mitigating harms, increased risk of harm, damaged credit, deprivation of the value of their Private Information, loss of privacy, and/or additional damages as described below.

10. In sum, Plaintiff and the Class will face an imminent risk of fraud and identity theft for the rest of their lives because (i) Digital Trust failed to protect Plaintiff's and the Class's PII, allowing a massive and preventable Data Breach to occur; (ii) the cybercriminals who perpetrated the Breach, stole Private Information that they will sell on the dark web; (iii) Digital Trust failed to provide any assurance that it paid a ransom to prevent Plaintiff's and the Class's data from being released on the dark web; and (iv) Digital Trust offered credit monitoring to Plaintiff and the Class, an offer it need not make if no PII was stolen and at risk of misuse.

11. Plaintiff brings this action individually and on behalf of the Class, seeking compensatory damages, punitive damages, nominal damages, restitution, and injunctive and declaratory relief, reasonable attorney fees and costs, and all other remedies this Court deems proper.

II. THE PARTIES

12. Plaintiff **Kevin Meagher** is an individual domiciled in Raleigh, North Carolina. Plaintiff

---

[6] *See* Exs. 1 and 2.

received a Notice of Data Breach Letter from Kingdom Trust dated August 21, 2024, notifying him that his Social Security number and name were "subject to unauthorized access."[7]

13. Defendant **Digital Trust, LLC f/k/a The Kingdom Trust Company** is a domestic Nevada limited liability company with a principal office address located at 7336 W. Post Road, Suite #111, Las Vegas, NV 89118. Defendant has members and/or managers domiciled in the State of Nevada. Defendant maintains and transacts substantial business across the state of Nevada.

III. JURISDICTION AND VENUE

14. This Court has subject matter jurisdiction pursuant to the Class Action Fairness Act of 2005 ("CAFA"), 28 U.S.C. §1332(d). The amount in controversy exceeds the sum of $5,000,000 exclusive of interest and costs, there are more than one hundred putative Class Members, and minimal diversity exists because many putative Class Members are citizens of a different state than Defendant.

15. This Court has personal jurisdiction over Defendant because Defendant is a Nevada domestic limited liability company; has its principal place of business in this District; conducts substantial business in this District through its headquarters, offices, and affiliates; engaged in the conduct at issue here in this District; and/or otherwise has substantial contacts with this District and purposely availed itself to the Courts in this District.

16. Venue is proper in this District under 28 U.S.C. §§ 1391(a)(2), 1391(b)(2), and 1391(c)(2) as a substantial part of the events giving rise to the claims emanated from activities within this District.

IV. FACTUAL ALLEGATIONS

A. Defendant and its Collection of Plaintiff's and the Class's PII.

17. "Digital Trust serves as an independent qualified custodian for the assets of clients of registered investment advisors, broker-dealers and investment sponsors, as well as their

---

[7] *See* Ex. 2.

Individual Retirement Accounts (IRAs), non-qualified plans and qualified defined contribution 401(k) plans."[8]

18. Digital Trust claims to provide "industry-leading technology to allow clients to have complete control over their Self-Directed IRA and other retirement and non-retirement accounts."[9]

19. In the Notice of Data Breach letter sent to Plaintiff and Class Members, Kingdom Trust claims it provides financial services to businesses, including The Loan Source, Inc. and ACAP SME, LLC, who provided services to Plaintiff and Class Members related to the U.S. Small Business Administration's Paycheck Protection Program.[10]

20. Digital Trust could have afforded to implement adequate data security prior to the Breach but deliberately chose not to.

21. In the ordinary course of business, Digital Trust receives the PII of individuals, such as Plaintiff and the Class, from the entities and individuals that utilize Digital Trust's services.

22. Digital Trust obtains, collects, uses, and derives a benefit from the PII of Plaintiff's and Class Members. Digital Trust uses the PII it collects to provide services, making a profit therefrom. Digital Trust would not be able to obtain revenue if not for the acceptance and use of Plaintiff's and the Class's PII.

23. By collecting Plaintiff's and the Class's PII, Digital Trust assumed legal and equitable duties to Plaintiff and the Class to protect and safeguard their PII from unauthorized access and intrusion.

24. Digital Trust recognizes this duty and makes the following claim on its website regarding its protection of sensitive data:

> **SECURITY**
> Digital Trust maintains a comprehensive disaster and security plan and a thorough set of controls and safeguards to ensure the security of our systems, website, data and real estate. The plan includes policies for operating the business as well as

---

[8] https://www.choiceapp.io/about-digital-trust.
[9] https://www.choiceapp.io/about-digital-trust.
[10] Exhibit 2.

> critical systems that need to be in place to conduct business. The plan is reviewed and tested annually to ensure all components are working properly and the systems will be functional in a timely manner if the need arises.[11]

25. Digital Trust's assurances of maintaining high standards of cybersecurity make it evident that Digital Trust recognized it had a duty to use reasonable measures to protect the PII that it collected and maintained.

26. Digital Trust violated its own privacy statement and failed to adopt reasonable and appropriate security practices and procedures including administrative, physical security, and technical controls to safeguard Plaintiff's and the Class's Private Information.

27. As a result, Plaintiff's and Class Members' PII was accessed and stolen from Digital Trust's inadequately secured data systems in a massive and preventable Data Breach.

B. Digital Trust's Massive and Preventable Data Breach.

28. On or around March 1, 2024, Kingdom Trust became aware of potential unauthorized access to its network.[12]

29. After detecting the Breach, Kingdom Trust claims it retained external cybersecurity professionals and notified law enforcement.[13]

30. Digital Trust specifically admitted "certain data was subject to unauthorized access" and that sensitive data "may have been copied from our network."[14]

31. The Private Information stolen in the Data Breach included at least: names and Social Security Numbers.[15]

32. Despite discovering the Data Breach on March 1, 2024, Digital Trust did not begin notifying individuals of the Data Breach until on or around August 1, 2024.[16]

33. In recognition of the severity of the Data Breach, and the imminent risk of harm Plaintiff and the Class face, Digital Trust made a measly offering of twelve (12) months of identity theft

---

[11] https://www.choiceapp.io/about-digital-trust.
[12] Ex. 2.
[13] *Id.*
[14] *Id.*; Ex. 1.
[15] Ex. 2.
[16] *Id.*

protection services.[17] Such an offering is inadequate and will not prevent identity theft but will only alert Data Breach victims once identity theft has ***already occurred***.

34. All in all, Digital Trust failed to take the necessary precautions required to safeguard and protect Plaintiff's and Class Members' PII from unauthorized access and exploitation.

35. Defendant's actions represent a flagrant disregard of the rights of Plaintiff and the Class, both as to privacy and property.

C. Cybercriminals Have Used and Will Continue to Use Plaintiff's and the Class's PII to Defraud Them.

36. PII is of great value to hackers and cybercriminals, and the data stolen in the Data Breach can and will be used in a variety of ways by criminals to exploit Plaintiff and the Class Members and to profit off their misfortune.

37. Each year, identity theft causes tens of billions of dollars of losses to victims in the United States.[18]

38. For example, with the PII stolen in the Data Breach, including Social Security numbers, identity thieves can open financial accounts, apply for credit, file fraudulent tax returns, commit crimes, create false driver's licenses and other forms of identification and sell them to other criminals or undocumented immigrants, steal government benefits, give breach victims' names to police during arrests, and many other harmful forms of identity theft.[19] These criminal activities have and will result in devastating financial and personal losses to Plaintiff and the Class Members.

39. Social security numbers are particularly sensitive pieces of personal information. As the

---

[17] *Id.*

[18] *Facts + Statistics: Identity Theft and Cybercrime*, INSURANCE INFO. INST., https://www.iii.org/fact-statistic/facts-statistics-identity-theft-and-cybercrime (discussing Javelin Strategy & Research's report "2018 Identity Fraud: Fraud Enters a New Era of Complexity").

[19] *See, e.g.*, Christine DiGangi, *What Can You Do with a Stolen Social Security Number*, CREDIT.COM (June 29, 2020), https://blog.credit.com/2017/11/5-things-an-identity-thief-can-do-with-your-social-security-number-108597/.

Consumer Federation of America explains:

> **Social Security number.** *This is the most dangerous type of personal information in the hands of identity thieves* because it can open the gate to serious fraud, from obtaining credit in your name to impersonating you to get medical services, government benefits, your tax refunds, employment – even using your identity in bankruptcy and other legal matters. It's hard to change your Social Security number and it's not a good idea because it is connected to your life in so many ways.[20]

[Emphasis added.]

40. PII is such a valuable commodity to identity thieves that once it has been compromised, criminals will use it for years.[21]

41. This was a financially motivated Breach, as the only reason the cybercriminals go through the trouble of running targeted cyberattacks against companies like Digital Trust is to get ransom money and/or information that they can monetize by selling on the black market for use in the kinds of criminal activity described herein.

42. Indeed, a social security number, date of birth, and full name can sell for $60 to $80 on the digital black market.[22]

43. "[I]f there is reason to believe that your personal information has been stolen, you should assume that it can end up for sale on the dark web."[23]

44. These risks are both certainly impending and substantial. As the Federal Trade Commission ("FTC") has reported, if hackers get access to PII, ***they will use it***.[24]

45. Hackers may not use the information right away, but this does not mean it will not be

---

[20] *Dark Web Monitoring: What You Should Know*, CONSUMER FEDERATION OF AMERICA (Mar. 19, 2019), https://consumerfed.org/consumer_info/dark-web-monitoring-what-you-should-know/.

[21] *Data Breaches Are Frequent, but Evidence of Resulting Identity Theft Is Limited; However, the Full Extent Is Unknown*, GAO, July 5, 2007, available at https://www.gao.gov/products/gao-07-737.

[22] Michael Kan, *Here's How Much Your Identity Goes for on the Dark Web* (Nov. 15, 2017), https://www.pcmag.com/news/heres-how-much-your-identity-goes-for-on-the-dark-web.

[23] *Dark Web Monitoring: What You Should Know*, CONSUMER FEDERATION OF AMERICA (Mar. 19, 2019), https://consumerfed.org/consumer_info/dark-web-monitoring-what-you-should-know/.

[24] Ari Lazarus, *How fast will identity thieves use stolen info?*, MILITARY CONSUMER (May 24, 2017), https://www.militaryconsumer.gov/blog/how-fast-will-identity-thieves-use-stolen-info.

used. According to the U.S. Government Accountability Office, which conducted a study regarding data breaches:

> [I]n some cases, stolen data may be held for up to a year or more before being used to commit identity theft. Further, once stolen data have been sold or posted on the Web, fraudulent use of that information ***may continue for years***. As a result, studies that attempt to measure the harm resulting from data breaches cannot necessarily rule out all future harm.[25]

46. For instance, with a stolen social security number, which is part of the PII compromised in the Data Breach, someone can open financial accounts, get medical care, file fraudulent tax returns, commit crimes, and steal benefits.[26]

47. With this Data Breach, identity thieves have already started to prey on the Digital Trust Data Breach victims, and we can anticipate that this will continue.

48. Identity theft victims must spend countless hours and large amounts of money repairing the impact to their credit as well as protecting themselves in the future.[27]

49. Defendant's offer of one year of identity monitoring to Plaintiff and the Class is woefully inadequate and will not fully protect Plaintiff from the damages and harm caused by its failures.

50. The full scope of the harm has yet to be realized. There may be a time lag between when harm occurs versus when it is discovered, and also between when PII is stolen and when it is used.

51. Once the twelve months have expired, Plaintiff and Class Members will need to pay for their own identity theft protection and credit monitoring for the rest of their lives due to Digital

---

[25] *Data Breaches Are Frequent, but Evidence of Resulting Identity Theft Is Limited; However, the Full Extent Is Unknown,* GAO (July 5, 2007), available at https://www.gao.gov/products/gao-07-737.

[26] *See, e.g.*, Christine DiGangi, *What Can You Do with a Stolen Social Security Number*, CREDIT.COM (June 29, 2020), https://blog.credit.com/2017/11/5-things-an-identity-thief-can-do-with-your-social-security-number-108597/.

[27] *Guide for Assisting Identity Theft Victims*, FEDERAL TRADE COMMISSION (Sept. 2013), *available at* https://www.global-screeningsolutions.com/Guide-for-Assisting-ID-Theft-Victims.pdf.

Trust's gross negligence.

52. Furthermore, identity monitoring only alerts someone to the fact that they have ***already been the victim of identity theft*** (*i.e.*, fraudulent acquisition and use of another person's PII)—it does not prevent identity theft.[28] Nor can an identity monitoring service remove personal information from the dark web.[29]

53. "The people who trade in stolen personal information [on the dark web] won't cooperate with an identity theft service or anyone else, so it's impossible to get the information removed, stop its sale, or prevent someone who buys it from using it."[30]

54. As a direct and proximate result of the Data Breach, Plaintiff and the Class have been damaged and have been placed at an imminent, immediate, and continuing increased risk of harm from continued fraud and identity theft. Plaintiff and the Class must now take the time and effort to mitigate the actual and potential impact of the Data Breach on their everyday lives, including placing "freezes" and "alerts" with credit reporting agencies, contacting their financial institutions, closing or modifying financial accounts, and closely reviewing and monitoring bank accounts and credit reports for unauthorized activity for years to come.

55. Even more seriously is the identity restoration that Plaintiff and other Class Members must go through, which can include spending countless hours filing police reports, filling out IRS forms, Federal Trade Commission checklists, Department of Motor Vehicle driver's license replacement applications, and calling financial institutions to cancel fraudulent credit applications, to name just a few of the steps Plaintiff and the Class must take.

56. Plaintiff and the Class have or will experience the following concrete and particularized

---

[28] *See, e.g.*, Kayleigh Kulp, *Credit Monitoring Services May Not Be Worth the Cost*, CNBC (Nov. 30, 2017, 9:00 AM), https://www.cnbc.com/2017/11/29/credit-monitoring-services-may-not-be-worth-the-cost.html.

[29] *Dark Web Monitoring: What You Should Know*, CONSUMER FEDERATION OF AMERICA (Mar. 19, 2019), https://consumerfed.org/consumer_info/dark-web-monitoring-what-you-should-know.

[30] *Id.*

harms for which they are entitled to compensation, including:

a. Actual identity theft;

b. Trespass, damage to, and theft of their personal property including PII;

c. Improper disclosure of their PII;

d. The imminent and certainly impending injury flowing from potential fraud and identity theft posed by their PII being placed in the hands of criminals;

e. Loss of privacy suffered as a result of the Data Breach, including the harm of knowing cyber criminals have their PII;

f. Ascertainable losses in the form of time taken to respond to identity theft and attempt to restore identity, including lost opportunities and lost wages from uncompensated time off from work;

g. Ascertainable losses in the form of out-of-pocket expenses and the value of their time reasonably expended to remedy or mitigate the effects of the Data Breach;

h. Ascertainable losses in the form of deprivation of the value of Plaintiff's and Class Members' Private Information for which there is a well-established and quantifiable national and international market;

i. The loss of use of and access to their credit, accounts, and/or funds;

j. Damage to their credit due to fraudulent use of their PII; and/or

k. Increased cost of borrowing, insurance, deposits, and the inability to secure more favorable interest rates because of a reduced credit score.

57. Moreover, Plaintiff and Class Members have an interest in ensuring that their Private Information, which remains in the possession of Defendant, is protected from further breaches by the implementation of industry standard security measures and safeguards. Defendant has shown itself wholly incapable of protecting Plaintiff's and the Class's Private Information.

58. Plaintiff and Class Members also have an interest in ensuring that their Private Information that was provided to Digital Trust is removed from all Digital Trust servers, systems, and files.

59. Defendant itself acknowledged the harm caused by the Data Breach because it offered

Plaintiff and Class Members woefully inadequate identity theft repair and monitoring services. Twelve months of identity theft and repair and monitoring is, however, inadequate to protect Plaintiff and Class Members from a lifetime of identity theft risk.

60. Defendant further acknowledged that the Data Breach would cause inconvenience to affected individuals and that financial harm would likely occur because it advised individuals to enroll in credit monitoring, place a fraud alert/security freeze on credit files, and obtain a free credit report.[31]

61. Alarmingly, Digital Trust did not assure Plaintiff and Class Members that it would improve its cyber security protocols after the Breach.

62. These enhanced protections should have been in place before the Data Breach.

63. At Digital Trust's suggestion, Plaintiff and the Class are desperately trying to mitigate the damage that Digital Trust has caused them.

64. Given the kind of Private Information Digital Trust made accessible to hackers, however, Plaintiff and the Class are certain to incur additional damages. Because identity thieves have their PII, Plaintiff and all Class Members will need to have identity theft monitoring protection for the rest of their lives. Some may even need to go through the long and arduous process of getting a new Social Security number, with all the loss of credit and employment difficulties that come with a new number.[32]

65. None of this should have happened because the Data Breach was entirely preventable.

D. Defendant was Aware of the Risk of Cyberattacks.

66. Data security breaches have dominated the headlines for the last two decades. And it doesn't take an IT industry expert to know it. The general public can tell you the names of some

---

[31] Ex. 2.

[32] *What happens if I change my Social Security number*, LEXINGTON LAW (Aug. 10, 2022), https://www.lexingtonlaw.com/blog/credit-101/will-a-new-social-security-number-affect-your-credit.html.

of the biggest cybersecurity breaches: Target,[33] Yahoo,[34] Marriott International,[35] Chipotle, Chili's, Arby's,[36] and others.[37]

67. Businesses in the financial services industry are prime targets because they provide cybercriminals with maximum impact and maximum profit.[38] Financial institutions, such as Defendant, perfectly meet these conditions because they store highly valuable data, and their digital transformation efforts are creating greater opportunities for cyber attackers to access that data.[39] This is why the financial sector is disproportionately targeted by cybercriminals, behind healthcare.[40]

68. In fact, in 2023, the financial sector suffered the most data breaches.[41]

69. The financial sector is an attractive target for cyber criminals not only for the immediate financial gain but also due to the wealth of sensitive customer information it holds.[42]

70. Digital Trust should certainly have been aware, and indeed was aware, that it was at risk of a data breach that could expose the PII that it collected and maintained.

71. Digital Trust was clearly aware of the risks it was taking and the harm that could result

---

[33] Michael Kassner, *Anatomy of the Target Data Breach: Missed Opportunities and Lessons Learned*, ZDNET (Feb. 2, 2015), https://www.zdnet.com/article/anatomy-of-the-target-data-breach-missed-opportunities-and-lessons-learned/.

[34] Martyn Williams, *Inside the Russian Hack of Yahoo: How They Did It*, CSOONLINE.COM (Oct. 4, 2017), https://www.csoonline.com/article/3180762/inside-the-russian-hack-of-yahoo-how-they-did-it.html.

[35] Patrick Nohe, *The Marriot Data Breach: Full Autopsy*, THE SSL STORE: HASHEDOUT (Mar. 22, 2019), https://www.thesslstore.com/blog/autopsying-the-marriott-data-breach-this-is-why-insurance-matters/ (last visited Oct. 9, 2023).

[36] Alfred Ng, *FBI Nabs Alleged Hackers in Theft of 15M Credit Cards from Chipotle, Others*, CNET (Aug. 1, 2018, 12:58 PM), https://www.cnet.com/news/fbi-nabs-alleged-hackers-in-theft-of-15m-credit-cards-from-chipotle-others/?ftag=CMG-01-10aaa1b.

[37] *See, e.g.*, Michael Hill and Dan Swinhoe, *The 15 Biggest Data Breaches of the 21st Century*, CSO ONLINE (Nov. 8, 2022), https://www.csoonline.com/article/2130877/the-biggest-data-breaches-of-the-21st-century.html.

[38] https://www.upguard.com/blog/biggest-data-breaches-financial-services.

[39] *Id.*

[40] *Id.*

[41] https://finance.yahoo.com/news/financial-industry-suffered-most-data-182214946.html.

[42] *Id.*

from inadequate data security but threw caution to the wind.

E. Digital Trust Could Have Prevented the Data Breach.

72. Data breaches are preventable.[43] As Lucy Thompson wrote in the DATA BREACH AND ENCRYPTION HANDBOOK, "In almost all cases, the data breaches that occurred could have been prevented by proper planning and the correct design and implementation of appropriate security solutions."[44] She added that "[o]rganizations that collect, use, store, and share sensitive personal data must accept responsibility for protecting the information and ensuring that it is not compromised . . . ."[45]

73. "Most of the reported data breaches are a result of lax security and the failure to create or enforce appropriate security policies, rules, and procedures. . . . Appropriate information security controls, including encryption, must be implemented and enforced in a rigorous and disciplined manner so that a *data breach never occurs*."[46]

74. In a data breach like this, many failures laid the groundwork for the Breach.

75. The FTC has published guidelines that establish reasonable data security practices for businesses.

76. The FTC guidelines emphasize the importance of having a data security plan, regularly assessing risks to computer systems, and implementing safeguards to control such risks.[47]

77. The FTC guidelines establish that businesses should protect the confidential information that they keep; properly dispose of personal information that is no longer needed; encrypt information stored on computer networks; understand their network's vulnerabilities; and

---

[43] Lucy L. Thomson, "Despite the Alarming Trends, Data Breaches Are Preventable," *in* DATA BREACH AND ENCRYPTION HANDBOOK (Lucy Thompson, ed., 2012), available at https://lawcat.berkeley.edu/record/394088.

[44] *Id.* at 17.

[45] *Id.* at 28.

[46] *Id.*

[47] *Protecting Personal Information: A Guide for Business*, FTC, available at https://www.ftc.gov/system/files/documents/plain-language/pdf-0136_proteting-personal-information.pdf.

implement policies for installing vendor-approved patches to correct security problems.

78. The FTC guidelines also recommend that businesses utilize an intrusion detection system to expose a breach as soon as it occurs; monitor all incoming traffic for activity indicating hacking attempts; watch for large amounts of data being transmitted from the system; and have a response plan ready in the event of a breach.

79. According to information and belief, Digital Trust failed to maintain many reasonable and necessary industry standards necessary to prevent a data breach, including the FTC's guidelines.

80. Upon information and belief, Digital Trust also failed to meet the minimum standards of any of the following frameworks: the NIST Cybersecurity Framework, NIST Special Publications 800-53, 53A, or 800-171; the Federal Risk and Authorization Management Program (FEDRAMP); or the Center for Internet Security's Critical Security Controls (CIS CSC), which are well respected authorities in reasonable cybersecurity readiness.

81. As explained by the Federal Bureau of Investigation, "[p]revention is the most effective defense against ransomware and it is critical to take precautions for protection."[48]

82. To prevent and detect malware attacks, including the malware attack that resulted in the Data Breach, Defendant could and should have implemented, as recommended by the Federal Bureau of Investigation, the following measures:

- Implement an awareness and training program. Because end users are targets, employees and individuals should be aware of the threat of ransomware and how it is delivered.
- Enable strong spam filters to prevent phishing emails from reaching the end users and authenticate inbound email using technologies like Sender Policy Framework (SPF), Domain Message Authentication Reporting and Conformance (DMARC),

---

[48] *See* How to Protect Your Networks from RANSOMWARE, at 3, available at https://www.fbi.gov/file-repository/ransomware-prevention-and-response-for-cisos.pdf/view.

and DomainKeys Identified Mail (DKIM) to prevent email spoofing.

- Scan all incoming and outgoing emails to detect threats and filter executable files from reaching end users.
- Configure firewalls to block access to known malicious IP addresses.
- Patch operating systems, software, and firmware on devices. Consider using a centralized patch management system.
- Set anti-virus and anti-malware programs to conduct regular scans automatically.
- Manage the use of privileged accounts based on the principle of least privilege: no users should be assigned administrative access unless absolutely needed; and those with a need for administrator accounts should only use them when necessary.
- Configure access controls—including file, directory, and network share permissions—with least privilege in mind. If a user only needs to read specific files, the user should not have write access to those files, directories, or shares.
- Disable macro scripts from office files transmitted via email. Consider using Office Viewer software to open Microsoft Office files transmitted via email instead of full office suite applications.
- Implement Software Restriction Policies (SRP) or other controls to prevent programs from executing from common ransomware locations, such as temporary folders supporting popular Internet browsers or compression/decompression programs, including the AppData/LocalAppData folder.
- Consider disabling Remote Desktop protocol (RDP) if it is not being used.
- Use application whitelisting, which only allows systems to execute programs known and permitted by security policy.
- Execute operating system environments or specific programs in a virtualized environment.
- Categorize data based on organizational value and implement physical and

logical separation of networks and data for different organizational units.[49]

83. Further, to prevent and detect malware attacks, Defendant could and should have implemented, as recommended by the United States Cybersecurity & Infrastructure Security Agency, the following measures:

- **Update and patch your computer.** Ensure your applications and operating systems (OSs) have been updated with the latest patches. Vulnerable applications and OSs are the target of most ransomware attacks….
- **Use caution with links and when entering website addresses**. Be careful when clicking directly on links in emails, even if the sender appears to be someone you know. Attempt to independently verify website addresses (e.g., contact your organization's helpdesk, search the internet for the sender organization's website or the topic mentioned in the email). Pay attention to the website addresses you click on, as well as those you enter yourself. Malicious website addresses often appear almost identical to legitimate sites, often using a slight variation in spelling or a different domain (e.g., .com instead of .net)….
- **Open email attachments with caution**. Be wary of opening email attachments, even from senders you think you know, particularly when attachments are compressed files or ZIP files.
- **Keep your personal information safe**. Check a website's security to ensure the information you submit is encrypted before you provide it….
- **Verify email senders**. If you are unsure whether or not an email is legitimate, try to verify the email's legitimacy by contacting the sender directly. Do not click on any links in the email. If possible, use a previous (legitimate) email to ensure the contact information you have for the sender is authentic before you contact

---

[49] *Id.* at 3–4.

them.

- **Inform yourself**. Keep yourself informed about recent cybersecurity threats and up to date on ransomware techniques. You can find information about known phishing attacks on the Anti-Phishing Working Group website. You may also want to sign up for CISA product notifications, which will alert you when a new Alert, Analysis Report, Bulletin, Current Activity, or Tip has been published.
- **Use and maintain preventative software programs**. Install antivirus software, firewalls, and email filters—and keep them updated—to reduce malicious network traffic….[50]

84. In addition, to prevent and detect ransomware attacks, including the ransomware attack that resulted in the Data Breach, Defendant could and should have implemented, as recommended by the Microsoft Threat Protection Intelligence Team, the following measures:

- **Secure internet-facing assets**
  - Apply latest security updates
  - Use threat and vulnerability management
  - Perform regular audit; remove privileged credentials
- **Thoroughly investigate and remediate alerts**
  - Prioritize and treat commodity malware infections as potential full compromise;
- **Include IT Pros in security discussions**
  - Ensure collaboration among [security operations], [security admins], and [information technology] admins to configure servers and other endpoints

---

[50] *See* Security Tip (ST19-001) Protecting Against Ransomware (original release date Apr. 11, 2019), available at https://www.cisa.gov/news-events/news/protecting-against-ransomware.

securely;

- **Build credential hygiene**
  - Use [multifactor authentication] or [network level authentication] and use strong, randomized, just-in-time local admin passwords
- **Apply principle of least-privilege**
  - Monitor for adversarial activities
  - Hunt for brute force attempts
  - Monitor for cleanup of Event Logs
  - Analyze logon events
- **Harden infrastructure**
  - Use Windows Defender Firewall
  - Enable tamper protection
  - Enable cloud-delivered protection
  - Turn on attack surface reduction rules and [Antimalware Scan Interface] for Office [Visual Basic for Applications].[51]

85. Given that Defendant was storing the PII of more than 6 million individuals, Defendant could have and should have implemented all of the above measures to prevent and detect cyberattacks.

86. Specifically, among other failures, Digital Trust had far too much confidential unencrypted information held on its systems. Such PII should have been segregated into an encrypted system.[52]

87. Moreover, it is a well-established industry standard practice for a business to dispose of

---

[51] *See* Human-operated ransomware attacks: A preventable disaster (Mar 5, 2020), *available at* https://www.microsoft.com/security/blog/2020/03/05/human-operated-ransomware-attacks-a-preventable-disaster/.

[52] *See, e.g.,* Adnan Raja, *How to Safeguard Your Business Data with Encryption*, FORTRA (Aug. 14, 2018), https://digitalguardian.com/blog/how-safeguard-your-business-data-encryption.

confidential PII once it is no longer needed.

88. The FTC, among others, has repeatedly emphasized the importance of disposing unnecessary PII, saying simply: "Keep sensitive data in your system only as long as you have a business reason to have it. Once that business need is over, properly dispose of it. If it's not on your system, it can't be stolen by hackers."[53] Digital Trust, rather than following this basic standard of care, kept thousands of individuals' unencrypted PII indefinitely.

89. In sum, the Data Breach could have readily been prevented through the use of industry standard network segmentation and encryption of all PII.

90. Further, the scope of the Data Breach could have been dramatically reduced had Digital Trust utilized proper record retention and destruction practices.

F. Plaintiff's Individual Experience

Plaintiff Kevin Meagher

91. Plaintiff Meagher received a Notice of Data Breach Letter from Defendant informing him that his highly confidential Private Information was compromised in the Data Breach.[54]

92. Defendant was in possession of Plaintiff's Private Information before, during, and after the Data Breach.

93. Because of the Data Breach, there is no doubt Plaintiff Meagher's highly confidential Private Information is in the hands of cybercriminals. Reason being, the Notice of Data Breach Letter from Defendant not only disclosed that an unauthorized third-party had accessed Defendant's systems, but it confirmed that the unauthorized criminal actor copied files containing highly sensitive PII.[55] As such, Plaintiff Meagher and the Class are at an imminent risk of identity theft and fraud.

94. As a result of the Data Breach, Plaintiff Meagher has already expended **10 hours** of his

---

[53] *Protecting Personal Information: A Guide for Business*, FTC, *available at* https://www.ftc.gov/system/files/documents/plain-language/pdf-0136_proteting-personal-information.pdf, at p. 6.

[54] Ex. 2.

[55] *Id.*

time and has suffered loss of productivity from taking time to address and attempt to ameliorate, mitigate, and address the future consequences of the Data Breach, including investigating the Data Breach, investigating how best to ensure that he is protected from identity theft, and reviewing account statements, credit reports, and/or other information. Additionally, Plaintiff has also placed a security freeze with two credit bureaus.

95. Plaintiff Meagher places significant value on the security of his Private Information and does not readily disclose it. Plaintiff Meagher has never knowingly transmitted unencrypted Private Information over the internet or any other unsecured source.

96. Plaintiff Meagher has been and will continue to be at a heightened and substantial risk of future identity theft and its attendant damages for years to come. Such a risk is certainly real and impending, and is not speculative, given the highly sensitive nature of the Private Information compromised by the Data Breach. Indeed, Defendant acknowledged the present and increased risk of future harm Plaintiff Meagher, and the Class now face by offering temporary, non-automatic credit monitoring services to Plaintiff Meagher and the Class.

97. Knowing that thieves intentionally targeted and stole his Private Information, including his Social Security number, and knowing that his Private Information is in the hands of cybercriminals has caused Plaintiff Meagher great anxiety beyond mere worry. Specifically, Plaintiff Meagher has lost hours of sleep, is in a constant state of stress, is very frustrated, and is in a state of persistent worry now that his Private Information has been stolen.

98. Plaintiff Meagher has a continuing interest in ensuring that his Private Information, which, upon information and belief, remains in the possession of Defendant, is protected, and safeguarded from future data breaches. Absent Court intervention, Plaintiff's and the Class's Private Information will be wholly unprotected and at-risk of future data breaches.

99. Plaintiff Meagher has suffered injuries directly and proximately caused by the Data Breach, including: (i) theft of his valuable Private Information; (ii) the imminent and certain impending injury flowing from anticipated fraud and identity theft posed by his Private Information being placed in the hands of cybercriminals; (iii) damages to and diminution in value of his Private Information that was entrusted to Defendant with the understanding that Defendant

would safeguard this information against disclosure; (iv) loss of the benefit of the bargain with Defendant to provide adequate and reasonable data security—*i.e.*, the difference in value between what Plaintiff Meagher should have received from Defendant and Defendant's defective and deficient performance of that obligation by failing to provide reasonable and adequate data security and failing to protect his Private Information; and (v) continued risk to his Private Information, which remains in the possession of Defendant and which is subject to further breaches so long as Defendant fails to undertake appropriate and adequate measures to protect the Private Information that was entrusted to Defendant.

V. CLASS ACTION ALLEGATIONS

100. Plaintiff incorporates by reference all preceding paragraphs as if fully restated here.

101. Plaintiff brings this action against Digital Trust on behalf of himself and all other individuals similarly situated under Federal Rule of Civil Procedure 23. Plaintiff asserts all claims on behalf of a nationwide class (the "Class") defined as follows:

> **All persons who were sent a Notice of Data Breach Letter from Kingdom Trust after the Data Breach**.

102. Excluded from the Class is Defendant, any entity in which Defendant has a controlling interest, and Defendant's officers, directors, legal representatives, successors, subsidiaries, and assigns. Also excluded from the Class is any judge, justice, or judicial officer presiding over this matter and members of their immediate families and judicial staff.

103. Plaintiff reserves the right to amend the above definition or to propose subclasses in subsequent pleadings and motions for class certification.

104. Plaintiff anticipates the issuance of notice setting forth the subject and nature of the instant action to the proposed Class. Upon information and belief, Defendant's own business records or electronic media can be utilized for the notice process.

105. The proposed Class meets the requirements of Federal Rule of Civil Procedure 23.

106. **Numerosity:** The proposed Class is so numerous that joinder of all members is impracticable.

107. **Typicality:** Plaintiff's claims are typical of the claims of the Class. Plaintiff and all

members of the Class were injured through Digital Trust's uniform misconduct. Digital Trust's inadequate data security gave rise to Plaintiff's claims and are identical to those that give rise to the claims of every other Class member because Plaintiff and each member of the Class had their sensitive PII compromised in the same way by the same conduct of Digital Trust.

108. **Adequacy:** Plaintiff is an adequate representative of the Class because Plaintiff's interests do not conflict with the interests of the Class; Plaintiff has retained counsel competent and highly experienced in data breach class action litigation; and Plaintiff and Plaintiff's counsel intend to prosecute this action vigorously. The interests of the Class will be fairly and adequately protected by Plaintiff and their counsel.

109. **Superiority:** A class action is superior to other available means of fair and efficient adjudication of the claims of Plaintiff and the Class. The injury suffered by each individual class member is relatively small in comparison to the burden and expense of individual prosecution of complex and expensive litigation. It would be very difficult if not impossible for members of the Class individually to effectively redress Digital Trust's wrongdoing. Even if Class members could afford such individual litigation, the court system could not. Individualized litigation presents a potential for inconsistent or contradictory judgments. Individualized litigation increases the delay and expense to all parties, and to the court system, presented by the complex legal and factual issues of the case. By contrast, the class action device presents far fewer management difficulties and provides benefits of single adjudication, economy of scale, and comprehensive supervision by a single court.

110. **Commonality and Predominance:** There are many questions of law and fact common to the claims of Plaintiff and the other members of the Class, and those questions predominate over any questions that may affect individual members of the Class. Common questions for the Class include:

a. Whether Defendant engaged in the wrongful conduct alleged herein;

b. Whether Defendant failed to adequately safeguard Plaintiff's and the Class's PII;

c. Whether Defendant owed a duty to Plaintiff and the Class to adequately protect

their PII, and whether it breached this duty;

d. Whether Digital Trust breached its duties to Plaintiff and the Class;

e. Whether Digital Trust failed to provide adequate cyber security;

f. Whether Digital Trust knew or should have known that its computer and network security systems were vulnerable to cyber-attacks;

g. Whether Digital Trust's conduct, including its failure to act, resulted in or was the proximate cause of the breach of its company network;

h. Whether Digital Trust was negligent in permitting unencrypted PII off vast numbers of individuals to be stored within its network;

i. Whether Digital Trust was negligent in failing to adhere to reasonable retention policies, thereby greatly increasing the size of the Data Breach;

j. Whether Digital Trust breached implied contractual duties to Plaintiff and the Class to use reasonable care in protecting their PII;

k. Whether Digital Trust failed to adequately respond to the Data Breach, including failing to investigate it diligently and notify affected individuals in the most expedient time possible and without unreasonable delay, and whether this caused damages to Plaintiff and the Class;

l. Whether Digital Trust continues to breach duties to Plaintiff and the Class;

m. Whether Plaintiff and the Class suffered injury as a proximate result of Digital Trust's negligent actions or failures to act;

n. Whether Plaintiff and the Class are entitled to recover damages, equitable relief, and other relief; and

o. Whether Digital Trust's actions alleged herein constitute gross negligence, and whether Plaintiff and Class Members are entitled to punitive damages.

////

////

////

////

VI. FIRST CAUSE OF ACTION
NEGLIGENCE
(On Behalf of Plaintiff and the Class)

111. Plaintiff incorporates paragraphs 1–110 as though fully set forth herein.

112. Digital Trust solicited, gathered, and stored the PII of Plaintiff and Class Members.

113. Upon accepting and storing the PII of Plaintiff and Class members on its computer systems and networks, Defendant undertook and owed a duty to Plaintiff and Class members to exercise reasonable care in obtaining, retaining, securing, safeguarding, deleting, and protecting the PII of Plaintiff and the Class from being compromised, lost, stolen, accessed, and misused by unauthorized persons.

114. Defendant had full knowledge of the sensitivity of the PII and the types of harm that Plaintiff and Class members could and would suffer if the PII was wrongfully disclosed. Plaintiff and Class members were the foreseeable victims of any inadequate safety and security practices. Plaintiff and the Class members had no ability to protect their PII that was in Defendant's possession. As such, a special relationship existed between Defendant and Plaintiff and the Class.

115. Because of this special relationship, Defendant required Plaintiff and Class members to provide their PII, including names, Social Security numbers, and other PII.

116. Implied in these exchanges was a promise by Defendant to ensure that the PII of Plaintiff and Class members in its possession was only used for the provided purpose and that Defendant would destroy any PII that it was not required to maintain.

117. As part of this special relationship, Defendant had a duty to perform with skill, care, and reasonable expedience and faithfulness.

118. Through Defendant's acts and omissions, including Defendant's failure to provide adequate data security, its failure to protect Plaintiff's and Class members' PII from being foreseeably accessed, and its improper retention of PII it was not required to maintain, Defendant negligently failed to observe and perform its duty.

119. Plaintiff and Class members did not receive the benefit of the bargain with Defendant, because providing their PII was in exchange for Defendant's implied agreement to secure and

keep it safe and to delete it once no longer required.

120. Defendant was aware of the fact that cybercriminals routinely target large corporations through cyberattacks in an attempt to steal customer and employee PII. In other words, Defendant knew of a foreseeable risk to its data security systems but failed to implement reasonable security measures.

121. Defendant owed Plaintiff and the Class members a common law duty to use reasonable care to avoid causing foreseeable risk of harm to Plaintiff and the Class when obtaining, storing, using, and managing personal information, including taking action to reasonably safeguard or delete such data and providing notification to Plaintiff and the Class members of any breach in a timely manner so that appropriate action could be taken to minimize losses.

122. Defendant's duty extended to protecting Plaintiff and the Class from the risk of foreseeable criminal conduct of third parties, which has been recognized in situations where the actor's own conduct or misconduct exposes another to the risk or defeats protections put in place to guard against the risk, or where the parties are in a special relationship. *See* Restatement (Second) of Torts § 302B.

123. Defendant had duties to protect and safeguard the PII of Plaintiff and the Class from being vulnerable to cyberattacks by taking common-sense precautions when dealing with sensitive PII. Additional duties that Defendant owed Plaintiff and the Class include:

a. To exercise reasonable care in designing, implementing, maintaining, monitoring, and testing Defendant's networks, systems, protocols, policies, procedures and practices to ensure that Plaintiff's and Class members' PII was adequately secured from impermissible release, disclosure, and publication;

b. To protect Plaintiff's and Class members' PII in its possession by using reasonable and adequate security procedures and systems;

c. To implement processes to quickly detect a data breach, security incident, or intrusion involving its networks and servers; and

d. To promptly notify Plaintiff and Class members of any data breach, security

incident, or intrusion that affected or may have affected their PII.

124. Plaintiff and the Class were the intended beneficiaries of Defendant's duties, creating a special relationship between them and Defendant. Defendant was in a position to ensure that its systems were sufficient to protect the PII that Plaintiff and the Class had entrusted to it.

125. Plaintiff's injuries and damages, as described herein, are a reasonably certain consequence of Defendant's negligence and breach of its duties.

126. Defendant breached its duties of care by failing to adequately protect Plaintiff's and Class members' PII. Defendant breached its duties by, among other things:

a. Failing to exercise reasonable care in obtaining, retaining securing, safeguarding, and protecting the PII in its possession;

b. Failing to protect the PII in its possession using reasonable and adequate security procedures and systems;

c. Failing to consistently enforce security policies aimed at protecting Plaintiff and the Class's PII;

d. Failing to implement processes to quickly detect data breaches, security incidents, or intrusions;

e. Failing to promptly notify Plaintiff and Class members of the Data Breach that affected their PII.

127. Defendant's willful failure to abide by these duties was wrongful, reckless, and grossly negligent considering the foreseeable risks and known threats.

128. As a direct and proximate result of Defendant's negligent conduct, including but not limited to its failure to implement and maintain reasonable data security practices and procedures as described above, Plaintiff and the Class have suffered damages and are at imminent risk of additional harms and damages (as alleged above).

129. Through Defendant's acts and omissions described herein, including but not limited to Defendant's failure to protect the PII of Plaintiff and Class members from being stolen and misused, Defendant unlawfully breached its duty to use reasonable care to adequately protect and secure the PII of Plaintiff and Class members while it was within Defendant's possession

and control.

130. Further, through its failure to provide timely and clear notification of the Data Breach to Plaintiff and Class members, Defendant prevented Plaintiff and Class members from taking meaningful, proactive steps to securing their PII and mitigating damages.

131. Plaintiff and Class members could have taken actions earlier had they been timely notified of the Data Breach.

132. Plaintiff and Class members could have enrolled in credit monitoring, could have instituted credit freezes, and could have changed their passwords, among other things, had they been alerted to the Data Breach more quickly.

133. Plaintiff and Class members have suffered harm from the delay in notifying them of the Data Breach.

134. As a direct and proximate cause of Defendant's conduct, including but not limited to its failure to implement and maintain reasonable security practices and procedures, Plaintiff and Class members have suffered, as Plaintiff have, and/or will suffer injury and damages, including but not limited to: (i) the loss of the opportunity to determine for themselves how their PII is used; (ii) the publication and/or theft of their PII; (iii) out-of-pocket expenses associated with the prevention, detection, and recovery from identity theft, tax fraud, and/or unauthorized use of their PII, including the need for substantial credit monitoring and identity protection services for an extended period of time; (iv) lost opportunity costs associated with effort expended and the loss of productivity addressing and attempting to mitigate the actual and future consequences of the Data Breach, including but not limited to efforts spent researching how to prevent, detect, contest and recover from tax fraud and identity theft; (v) costs associated with placing freezes on credit reports and password protections; (vi) anxiety, emotional distress, loss of privacy, and other economic and non-economic losses; (vii) the continued risk to their PII, which remains in Defendant's possession and is subject to further unauthorized disclosures so long as Defendant fails to undertake appropriate and adequate measures to protect the PII of employees in its continued possession; and, (viii) future costs in terms of time, effort and money that will be expended to prevent, detect, contest, and repair the inevitable and continuing consequences of

compromised PII for the rest of their lives. Thus, Plaintiff and the Class are entitled to damages in an amount to be proven at trial.

135. The damages Plaintiff and the Class have suffered (as alleged above) and will suffer were and are the direct and proximate result of Defendant's negligent conduct.

136. Plaintiff and the Class have suffered injury and are entitled to actual and punitive damages in an amount to be proven at trial.

VII. SECOND CAUSE OF ACTION
NEGLIGENCE *PER SE*
(On Behalf of Plaintiff and the Class)

137. Plaintiff incorporates paragraphs 1–136 as though fully set forth herein.

138. Pursuant to the FTC Act, 15 U.S.C. § 45(a), Defendant had a duty to Plaintiff and the Class to provide fair and adequate computer systems and data security to safeguard the PII of Plaintiff and the Class.

139. The FTC Act prohibits "unfair practices in or affecting commerce," including, as interpreted and enforced by the FTC, the unfair act or practice by businesses, such as Defendant, of failing to use reasonable measures to protect PII. The FTC publications and orders described above also formed part of the basis of Defendant's duty in this regard.

140. Defendant gathered and stored the PII of Plaintiff and the Class as part of their business which affects commerce.

141. Defendant violated the FTC Act by failing to use reasonable measures to protect the PII of Plaintiff and the Class and by not complying with applicable industry standards, as described herein.

142. Defendant breached its duties to Plaintiff and the Class under the FTC Act by failing to provide fair, reasonable, or adequate computer systems and/or data security practices to safeguard Plaintiff's and Class members' PII, and by failing to provide prompt notice without reasonable delay.

143. Defendant's multiple failures to comply with applicable laws and regulations constitutes negligence *per se*.

144. Plaintiff and the Class are within the class of persons that the FTC Act was intended to

protect.

145. The harm that occurred as a result of the Data Breach is the type of harm the FTC Act was intended to guard against.

146. Defendant breached its duties to Plaintiff and the Class under the FTC Act by failing to provide fair, reasonable, or adequate computer systems and data security practices to safeguard Plaintiff's and the Class's PII.

147. Defendant breached its duties to Plaintiff and the Class by unreasonably delaying and failing to provide notice of the Data Breach expeditiously and/or as soon as practicable to Plaintiff and the Class.

148. Defendant's violations of the FTC Act constitute negligence *per se*.

149. As a direct and proximate result of Defendant's negligence *per se*, Plaintiff and the Class have suffered, and continue to suffer, damages arising from the Data Breach, as alleged above.

150. The injury and harm that Plaintiff and Class members suffered (as alleged above) was the direct and proximate result of Defendant's negligence *per se*.

151. Plaintiff and the Class have suffered injury and are entitled to damages in amounts to be proven at trial.

VIII. THIRD CAUSE OF ACTION
BREACH OF THIRD-PARTY BENEFICIARY CONTRACT
(On Behalf of Plaintiff and the Class)

152. Plaintiff incorporates paragraphs 1–151 as though fully set forth herein.

153. On information and belief, Defendant entered into written contracts to provide financial services to companies.

154. In exchange, Defendant agreed, in part, to implement adequate security measures to safeguard the PII of Plaintiff and the Class and to timely and adequately notify them of the Data Breach.

155. According to information and belief, these contracts were made expressly for the benefit of Plaintiff and the Class, as Plaintiff and Class Members were the intended third-party beneficiaries of the contracts entered into between Defendant and its clients. Defendant knew that, if it were to breach these contracts with its clients, Plaintiff and Class Members would be

harmed.

156. Defendant breached the contracts entered into with its clients by, among other things, failing to (i) use reasonable data security measures, (ii) implement adequate protocols and employee training sufficient to protect Plaintiff's and Class Members' Private Information from unauthorized disclosure to third parties, and (iii) promptly and adequately notify Plaintiff and Class Members of the Data Breach.

157. Plaintiff and the Class were harmed by Defendant's breaches of contract, as such breach is alleged herein, and are entitled to the losses and damages they have sustained as a direct and proximate result thereof.

158. Plaintiff and Class Members are also entitled to their costs and attorney's fees incurred in this action.

IX. FOURTH CAUSE OF ACTION
UNJUST ENRICHMENT
(On Behalf of Plaintiff and the Class)

159. Plaintiff incorporates paragraphs 1–159 as though fully set forth herein.

160. Plaintiff alleges this claim in the alternative to his breach of third-party beneficiary contract claim.

161. Defendant knew that Plaintiff and Class Members conferred a benefit upon it and accepted and retained that benefit by accepting and retaining the PII entrusted to it. Defendant profited from Plaintiff's retained data and commercialized and used Plaintiff's and Class Members' PII for business purposes.

162. Upon information and belief, Defendant funds its data security measures entirely from its general revenue, including payments on behalf of or for the benefit of Plaintiff and Class Members.

163. As such, a portion of the payments made for the benefit of or on behalf of Plaintiff and Class Members is to be used to provide a reasonable level of data security, and the amount of the portion of each payment made that is allocated to data security is known to Defendant.

164. Defendant failed to secure Plaintiff's and Class Members' Private Information and, therefore, did not fully compensate Plaintiff or Class Members for the value that their PII

provided.

165. Defendant acquired the PII through inequitable means as it failed to disclose the inadequate data security practices previously alleged. If Plaintiff and Class Members had known that Defendant would not fund adequate data security practices, procedures, and protocols to sufficiently monitor, supervise, and secure their PII, they would not have entrusted their Private Information to Defendant or obtained services from Defendant's clients.

166. Defendant enriched itself by saving the costs it reasonably should have expended on data security measures to secure Plaintiff's and Class Members' PII. Instead of providing a reasonable level of security that would have prevented the Data Breach, Defendant instead calculated to increase its own profits at the expense of Plaintiff and Class Members by utilizing cheaper, ineffective security measures and diverting those funds to their own benefit. Plaintiff and Class Members, on the other hand, suffered as a direct and proximate result of Defendant's decision to prioritize its own profits over the requisite security and the safety of their PII.

167. Plaintiff and Class Members have no adequate remedy at law.

168. Under the circumstances, it would be unjust for Defendant to be permitted to retain any of the benefits that Plaintiff and Class Members conferred upon it.

169. As a direct and proximate result of Defendant's conduct, Plaintiff and other Class Members, have suffered actual harm in the form of experiencing specific acts of fraudulent activity and other attempts of fraud that required Plaintiff' efforts to prevent from succeeding.

170. As a result of Defendant's wrongful conduct, as alleged above, Plaintiff and the Class are entitled to restitution and disgorgement of profits, benefits, and other compensation obtained by Defendant and all other relief allowed by law.

X. FIFTH CAUSE OF ACTION
DECLARATORY AND INJUNCTIVE RELIEF
(On Behalf of Plaintiff and the Class)

171. Plaintiff incorporates paragraphs 1–170 as though fully set forth herein.

172. This count is brought under the Federal Declaratory Judgment Act, 28 U.S.C. § 2201.

173. As previously alleged, Plaintiff and members of the Class are entered into implied contracts with Defendant, which contracts required Defendant to provide adequate security for

the PII collected from Plaintiff and the Class.

174. Defendant owed and still owes a duty of care to Plaintiff and Class members that require it to adequately secure Plaintiff's and Class members' PII.

175. Upon reason and belief, Defendant still possesses the PII of Plaintiff and the Class members.

176. Defendant has not satisfied its contractual obligations and legal duties to Plaintiff and the Class members.

177. Since the Data Breach, Defendant has not yet announced any changes to its data security infrastructure, processes or procedures to fix the vulnerabilities in its computer systems and/or security practices which permitted the Data Breach to occur and go undetected and, thereby, prevent further attacks.

178. Defendant has not satisfied its contractual obligations and legal duties to Plaintiff and the Class. In fact, now that Defendant's insufficient data security is known to hackers, the PII in Defendant's possession is even more vulnerable to cyberattack.

179. Actual harm has arisen in the wake of the Data Breach regarding Defendant's contractual obligations and duties of care to provide security measures to Plaintiff and the members of the Class. Further, Plaintiff and the members of the Class are at risk of additional or further harm due to the exposure of their PII and Defendant's failure to address the security failings that led to such exposure.

180. There is no reason to believe that Defendant's security measures are any more adequate now than they were before the Data Breach to meet Defendant's contractual obligations and legal duties.

181. Plaintiff and the Class, therefore, seek a declaration (1) that Defendant's existing security measures do not comply with its contractual obligations and duties of care to provide adequate security, and (2) that to comply with its contractual obligations and duties of care, Defendant must implement and maintain reasonable security measures, including, but not limited to:

a. Ordering that Defendant engage third-party security auditors/penetration testers as well as internal security personnel to conduct testing, including simulated

attacks, penetration tests, and audits on Defendant's systems on a periodic basis, and ordering Defendant to promptly correct any problems or issues detected by such third-party security auditors;

b. Ordering that Defendant engage third-party security auditors and internal personnel to run automated security monitoring;

c. Ordering that Defendant audit, test, and train its security personnel regarding any new or modified procedures;

d. Ordering that Defendant segment employee data by, among other things, creating firewalls and access controls so that if one area of Defendant's systems is compromised, hackers cannot gain access to other portions of Defendant's systems;

e. Ordering that Defendant purge, delete, and destroy, in a reasonably secure manner, customer data not necessary for their provisions of services;

f. Ordering that Defendant conduct regular database scanning and security checks; and

g. Ordering that Defendant routinely and continually conduct internal training and education to inform internal security personnel how to identify and contain a breach when it occurs and what to do in response to a breach.

XI. PRAYER FOR RELIEF

WHEREFORE, Plaintiff and the Class pray for judgment against Defendant as follows:

a. An order certifying this action as a class action under Federal Rule of Civil Procedure 23, defining the Class as requested herein, appointing the undersigned as Class counsel, and finding that Plaintiff are proper representatives of the Class requested herein;

b. A judgment in favor of Plaintiff and the Class awarding them appropriate monetary relief, including compensatory damages, punitive damages, attorney fees, expenses, costs, and such other and further relief as is just and proper;

c. An order providing injunctive and other equitable relief as necessary to protect

the interests of the Class as requested herein;

d. An order requiring Defendant to pay the costs involved in notifying the Class Members about the judgment and administering the claims process;

e. A judgment in favor of Plaintiff and the Class awarding them pre-judgment and post-judgment interest, reasonable attorneys' fees, costs, and expenses as allowable by law; and

f. An award of such other and further relief as this Court may deem just and proper.

Dated: September 4, 2024

LEVERTY AND ASSOCIATES LAW, CHTD.

Patrick R. Leverty, NV Bar No. 8840
William R. Ginn, NV Bar No. 6869
832 Willow Street
Reno, NV 89502

FEDERMAN & SHERWOOD

William B. Federman
(pro hac vice application forthcoming)
Kennedy M. Brian
(pro hac vice application forthcoming)
FEDERMAN & SHERWOOD
10205 N. Pennsylvania Ave.
Oklahoma City, OK 73120

Attorneys for Plaintiff Class